PROBLEMS IN CODED COMMUNICATIONS: PERFORMANCE BOUNDS AND POLAR CODING

Eran Hof

Supervised by

Igal Sason and Shlomo Shamai

Outline

- Performance bounds
  - Non-binary linear block codes under ML decoding
  - Binary and non-binary linear block codes under generalized decoding rules
- Polar coding
  - Wire-tap channel
  - Parallel channels with arbitrary input-permutation

Performance analysis of coded communication systems

- Upper and lower bounds on the decoding error probability are interesting as both theoretical and engineering tools
- Union bounds are useless at rates exceeding the channel cut-off rate
- Modern coding schemes perform reliably at rates close to the capacity

A bounding tour

- Gallager
  - Fully random block code ensembles
  - Informative at all rates below capacity
- Duman and Salehi
  - Structured codes and code ensembles
  - DS2 and generalizations for various memoryless channels
  - Facilitates the derivation of previously reported bounds
- Shulman and Feder
  - Structured codes and code ensembles
  - Coincides with Gallager's random coding bound
  - Non-binary adaptations
- Sphere Packing lower bounds

New results

- **Chapter 2:** "Performance bounds for non-binary linear block codes over memoryless symmetric channels," *IEEE Trans. on Information Theory, vol. 55, no. 3, pp. 977–996, March 2009.*
- **Chapter 3:** "Performance Bounds for Erasure, List and Decision Feedback Schemes with Linear Block Codes," *IEEE Trans. on Information Theory, vol. 56, no. 8, pp. 3754–3778, August 2010.*

Non-binary linear block codes under ML decoding

- Message independence proposition for memoryless symmetric channels
- Adaptation of Gallager's'65 technique for structured codes or ensembles
  - Adapt the DS2 bound for non-binary codes
  - Derivation of particular bounds which are easy to calculate and provide some insight to the problem.
- Applications for the non-binary regular LDPC ensembles of Gallager
  - A derivation of the exact complete composition spectra
  - A comparison to the ultimate code performance (SP59, ISP)
  - Transmissions over various memoryless channel models

Memoryless symmetric channels

Definition (discrete memoryless channels)

Input-alphabet $\mathcal{X}$

Output alphabet $\mathcal{Y}$

transition probability p

$$\exists \ \mathcal{T} : \mathcal{Y} \times \mathcal{X} \to \mathcal{Y}$$

1. $\mathcal{T}(\cdot, x) : \mathcal{Y} \to \mathcal{Y}$ is bijective
2. $p(y|x_1) = p(\mathcal{T}(y, x_2 - x_1)|x_2)$

Particular cases

- Continuous-output alphabet
- MBIOS channels

$$\mathcal{T}(y,x) = \begin{cases} y & x = 0 \\ -y & x = 1 \end{cases}$$

- Coding schemes with a random coset mechanism

$$\mathcal{T}((y,v),x) = (y, v - x), \quad y \in \mathcal{Y},\ x, v \in \mathcal{X}$$

Message independence

Proposition

- A1. Linear block codes
- A2. Memoryless symmetric channels

The block error probability under ML decoding is independent on the transmitted message.

Example

Gallager's symmetry does not guarantee message independence

The DS2 bound

$$P_{\mathrm{e}|m} \leq \left(\sum_{\mathbf{y} \in \mathcal{Y}^n} G_n^m(\mathbf{y}) p_n(\mathbf{y}|\mathbf{x}_m) \right)^{1-\rho}$$

$$\cdot \left\{ \sum_{m' \neq m} \sum_{\mathbf{y} \in \mathcal{Y}^n} G_n^m(\mathbf{y})^{1-\frac{1}{\rho}} p_n(\mathbf{y}|\mathbf{x}_m) \left(\frac{p_n(\mathbf{y}|\mathbf{x}_{m'})}{p_n(\mathbf{y}|\mathbf{x}_m)} \right)^{\lambda} \right\}^{\rho}$$

Theorem (Non-binary Shulman-Feder)

$$P_{\mathrm{e}} \leq \; q^{-nE_{\mathrm{r}}\left(R + \frac{\log_q \alpha(\mathcal{C})}{n}\right)}$$

$$\alpha(\mathcal{C}) \triangleq \max_{\mathbf{t} \in \mathcal{T}^*} \left\{ \frac{\mathsf{E}\left[\left| \mathcal{C}_{\mathbf{t}} \right| \right]}{q^{-n(1-R)} \binom{n}{\mathbf{t}}} \right\}$$

Ensemble symmetry

$$\mathsf{E}\left[|\mathcal{C}_{\mathbf{t}}|\right] = P(n-t_0)\binom{n}{\mathbf{t}}$$

Theorem

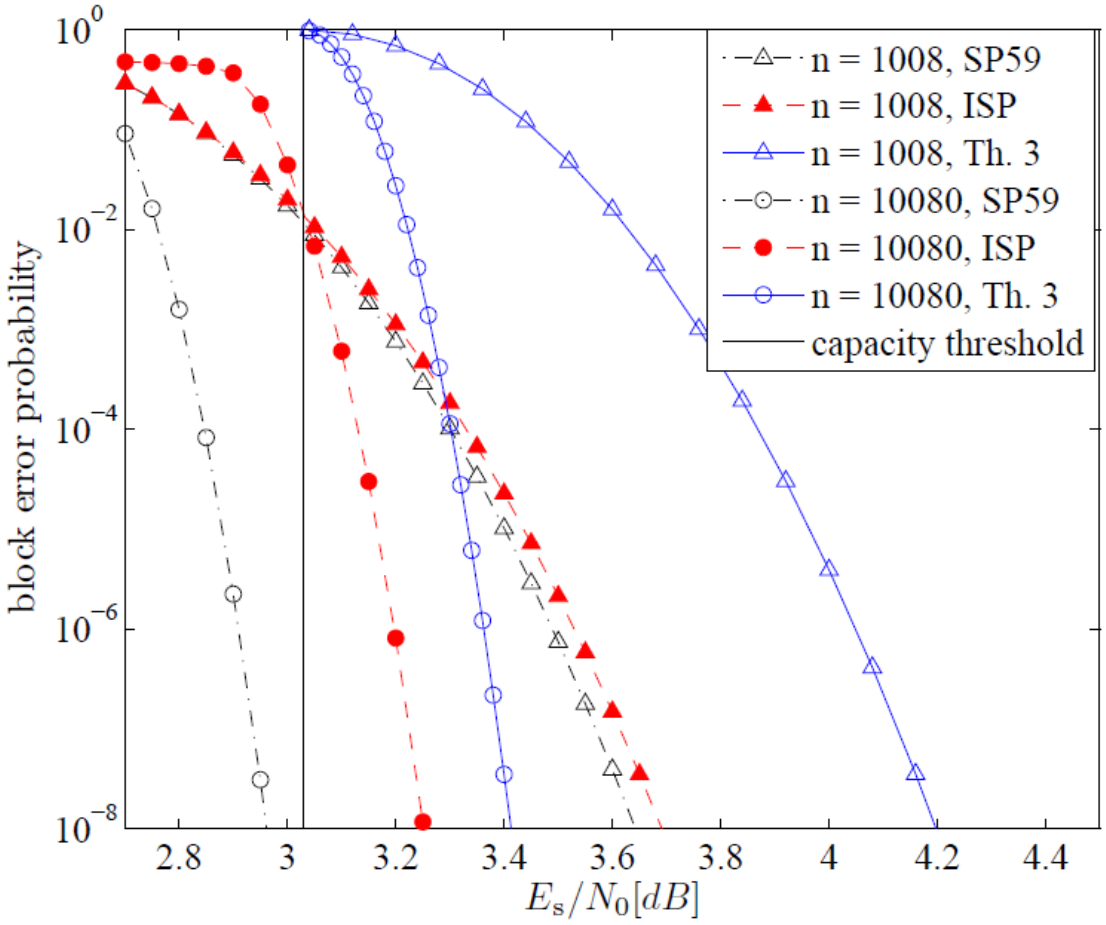
$$P_{\mathrm{e}} \leq A(\rho)^{n(1-\rho)}\left(\sum_{l}\left(P(l)\binom{n}{l}B(\rho)^{n-l}C(\rho)^{l}\right)\right)^{\rho}$$

$$A(\rho) \triangleq \sum_{y\in\mathcal{Y}}\left(\frac{1}{q}\sum_{x\in\mathcal{X}}p(y|x)^{\frac{1}{1+\rho}}\right)^{1+\rho}$$

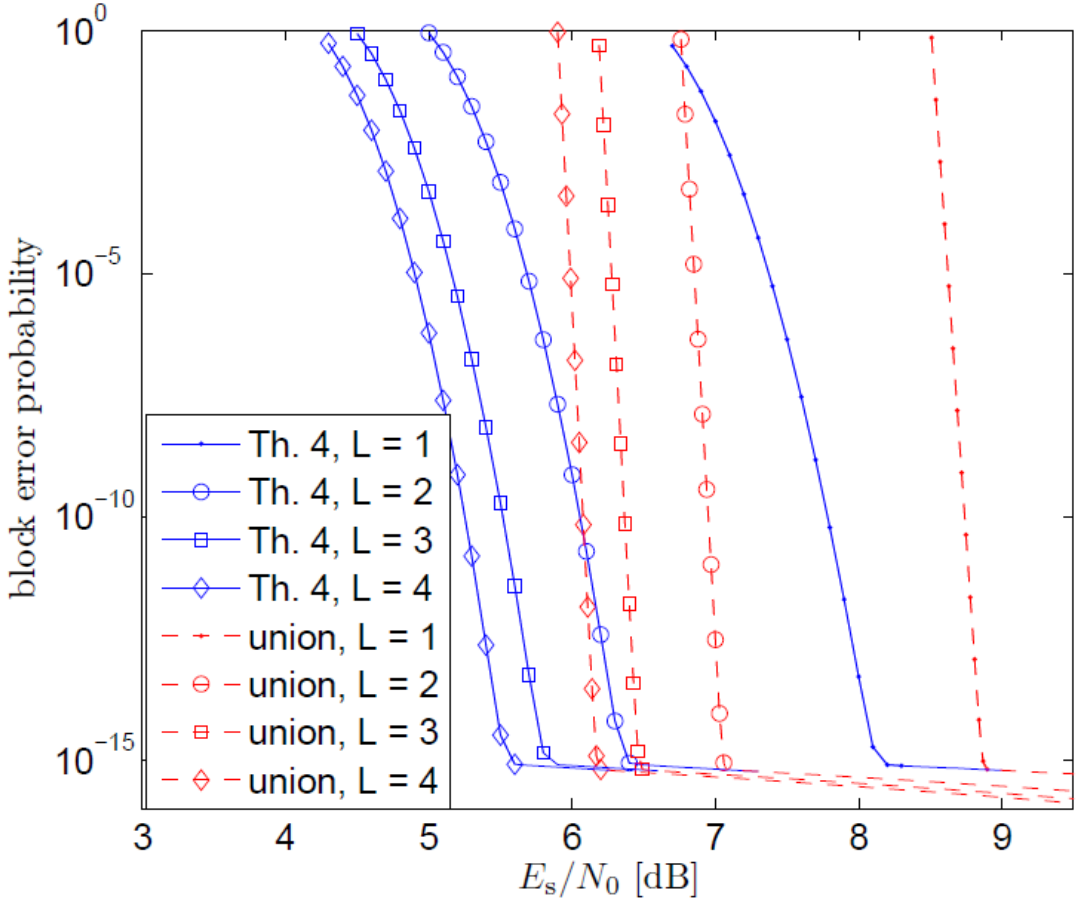
$$B(\rho) \triangleq \sum_{y\in\mathcal{Y}}\left(\frac{1}{q}\sum_{x\in\mathcal{X}}p(y|x)^{\frac{1}{1+\rho}}\right)^{\rho-1}\left(\frac{1}{q}\sum_{x\in\mathcal{X}}p(y|x)^{\frac{2}{1+\rho}}\right)$$

$$C(\rho) \triangleq qA(\rho) - B(\rho)$$

Example


block error probability
10^{0}
10^{-2}
10^{-4}
10^{-6}
10^{-8}
2.8
3
3.2
3.4
3.6
3.8
4
4.2
4.4
$E_s/N_0[dB]$
n = 1008, SP59
n = 1008, ISP
n = 1008, Th. 3
n = 10080, SP59
n = 10080, ISP
n = 10080, Th. 3
capacity threshold

Example


block error probability
10^{0}
10^{-5}
10^{-10}
10^{-15}
3
4
5
6
7
8
9
E_s/N_0 [dB]
Th. 4, L = 1
Th. 4, L = 2
Th. 4, L = 3
Th. 4, L = 4
union, L = 1
union, L = 2
union, L = 3
union, L = 4

Binary and non-binary linear block codes under generalized decoding rules

- Generalized decoding rules
  - Forney's optimal decoding rule with erasure and list decoding
  - LR test decoding
  - Fixed-size list decoding
- Message independence properties for linear block codes
- Performance bounds
  - Gallager type (DS2)
  - Error exponents
  - Finite block length analysis

Generalized decoding

206 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-14, NO. 2, MARCH 1968

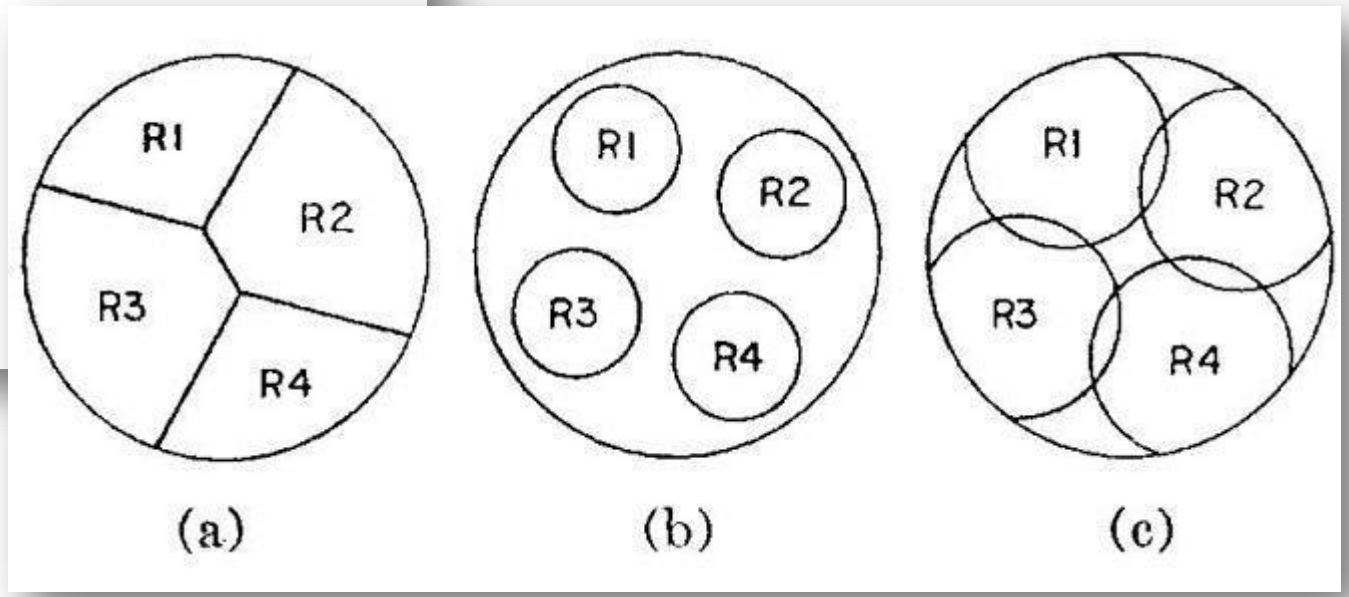
Exponential Error Bounds for Erasure, List, and Decision Feedback Schemes

G. DAVID FORNEY, JR., MEMBER, IEEE

Abstract—By an extension of Gallager's bounding methods, exponential error bounds applicable to coding schemes involving erasures, variable-size lists, and decision feedback are obtained. The bounds are everywhere the tightest known.

Introduction

ONE of the central problems of coding theory is the question of the error probability obtainable by coding on memoryless channels. Coding theory's first result, and still its most important, was Shannon's[1] proof that every memoryless channel has a capacity C, such that arbitrarily small error probabilities can be obtained if and only if the code rate R is less than C. Many years of continuing attempts to make more precise statements about error probabilities[2] culminated in Gallager's elegant derivation[3] of an exponential upper bound on attainable error probabilities, and in a nearly identical lower bound.[4]



206 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-14, NO. 2, MARCH 1968

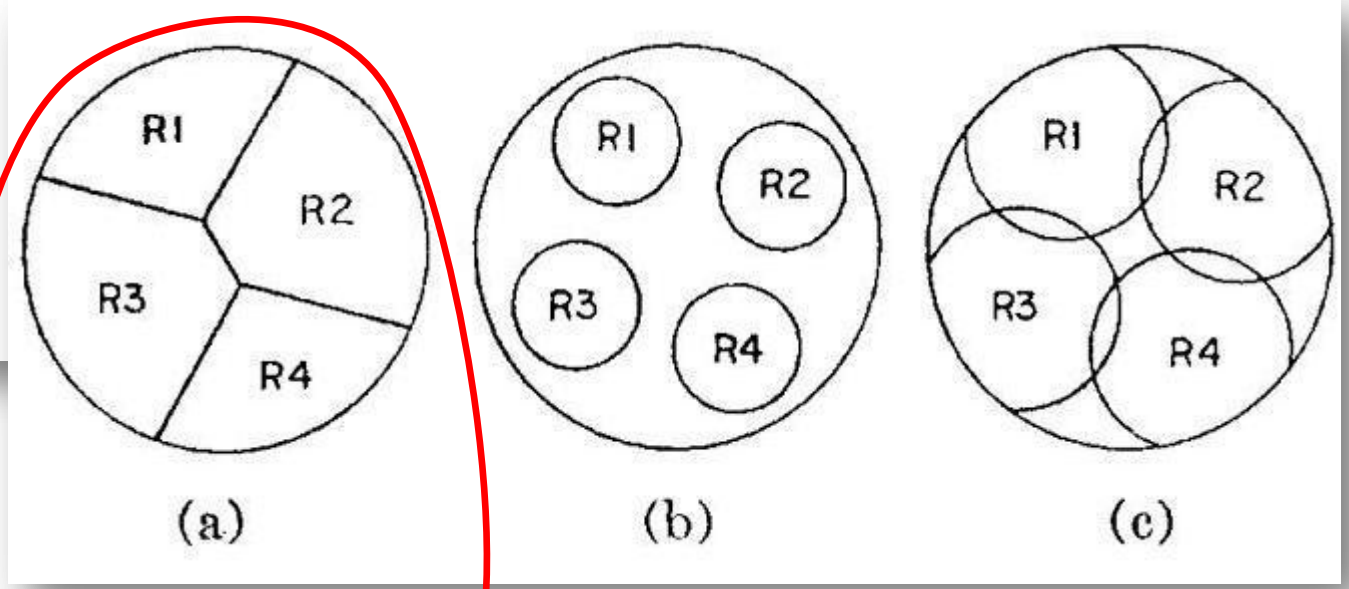
Exponential Error Bounds for Erasure, List, and Decision Feedback Schemes

G. DAVID FORNEY, JR., MEMBER, IEEE

Abstract—By an extension of Gallager's bounding methods, exponential error bounds applicable to coding schemes involving erasures, variable-size lists, and decision feedback are obtained. The bounds are everywhere the tightest known.

Introduction

ONE of the central problems of coding theory is the question of the error probability obtainable by coding on memoryless channels. Coding theory's first result, and still its most important, was Shannon's[1] proof that every memoryless channel has a capacity C, such that arbitrarily small error probabilities can be obtained if and only if the code rate R is less than C. Many years of continuing attempts to make more precise statements about error probabilities[2] culminated in Gallager's elegant derivation[3] of an exponential upper bound on attainable error probabilities, and in a nearly identical lower bound.[4]



$$\Lambda_m \bigcap \Lambda_k = \emptyset$$
$$\bigcup_m \Lambda_m = \mathcal{Y}^n$$

Generalized decoding

206 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-14, NO. 2, MARCH 1968

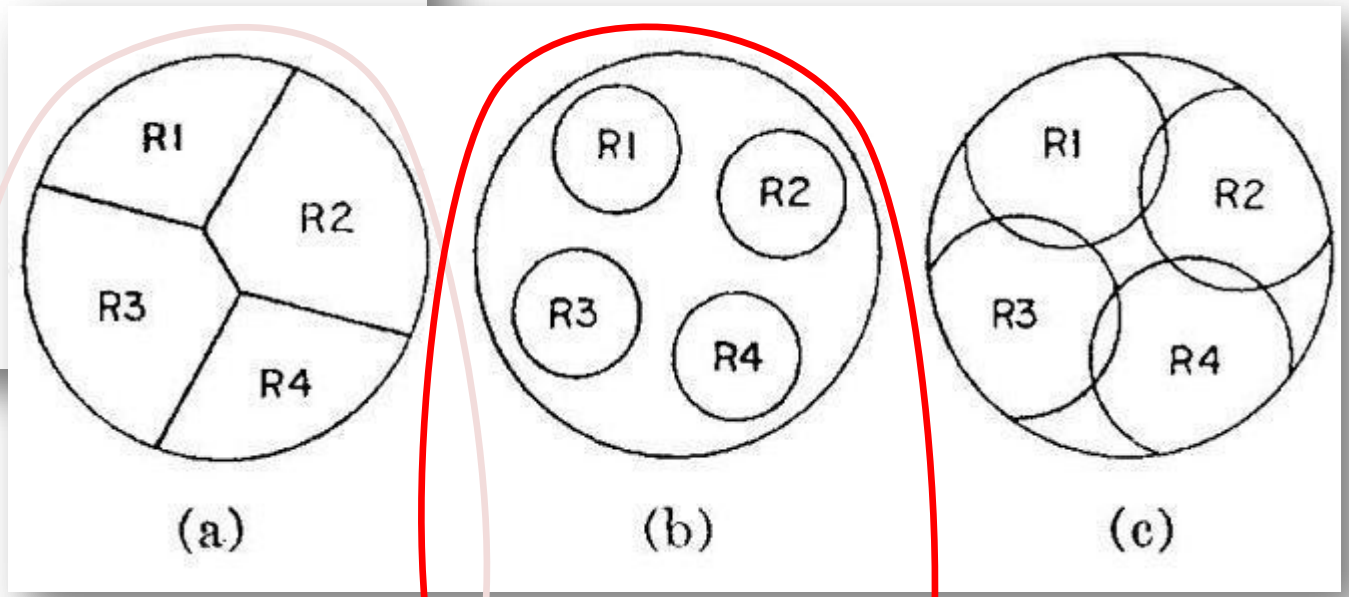
Exponential Error Bounds for Erasure, List, and Decision Feedback Schemes

G. DAVID FORNEY, JR., MEMBER, IEEE

Abstract—By an extension of Gallager's bounding methods, exponential error bounds applicable to coding schemes involving erasures, variable-size lists, and decision feedback are obtained. The bounds are everywhere the tightest known.

Introduction

ONE of the central problems of coding theory is the question of the error probability obtainable by coding on memoryless channels. Coding theory's first result, and still its most important, was Shannon's[1] proof that every memoryless channel has a capacity C, such that arbitrarily small error probabilities can be obtained if and only if the code rate R is less than C. Many years of continuing attempts to make more precise statements about error probabilities[2] culminated in Gallager's elegant derivation[3] of an exponential upper bound on attainable error probabilities, and in a nearly identical lower bound.[4]



$$\Lambda_m \bigcap \Lambda_k = \emptyset$$
$$\bigcup_m \Lambda_m = \mathcal{Y}^n$$

$$\Lambda_m \bigcap \Lambda_k = \emptyset$$
$$\bigcup_m \Lambda_m \subseteq \mathcal{Y}^n$$

206 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-14, NO. 2, MARCH 1968

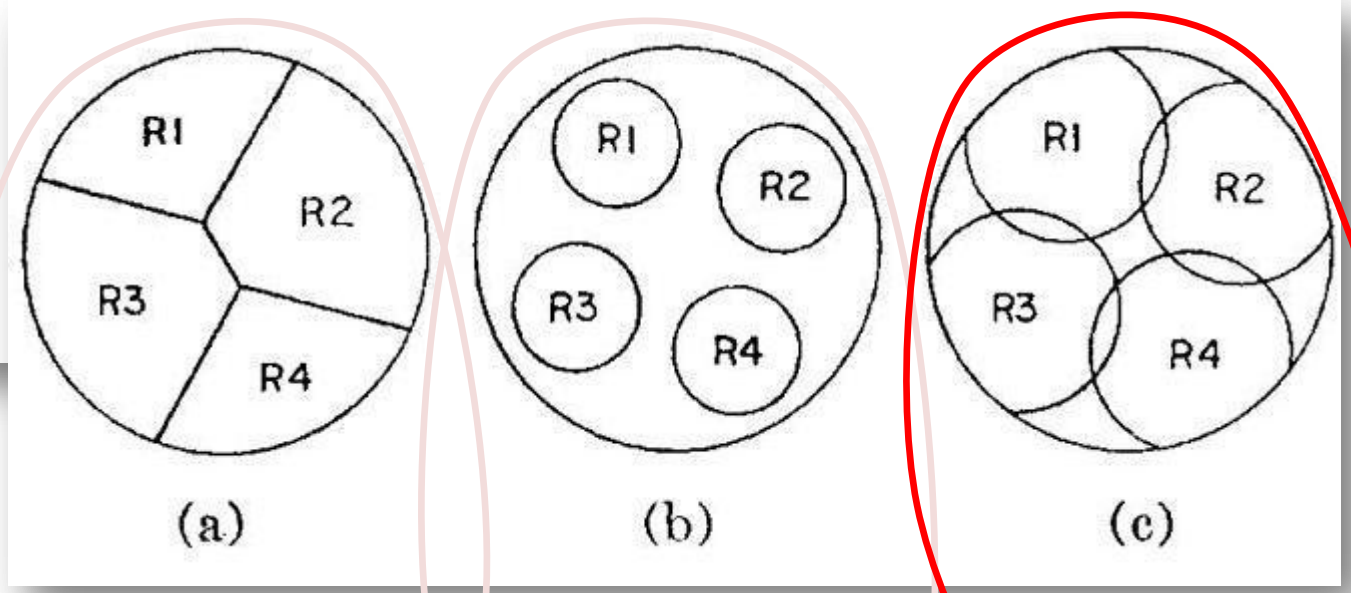
Exponential Error Bounds for Erasure, List, and Decision Feedback Schemes

G. DAVID FORNEY, JR., MEMBER, IEEE

Abstract—By an extension of Gallager's bounding methods, exponential error bounds applicable to coding schemes involving erasures, variable-size lists, and decision feedback are obtained. The bounds are everywhere the tightest known.

Introduction

ONE of the central problems of coding theory is the question of the error probability obtainable by coding on memoryless channels. Coding theory's first result, and still its most important, was Shannon's[1] proof that every memoryless channel has a capacity C, such that arbitrarily small error probabilities can be obtained if and only if the code rate R is less than C. Many years of continuing attempts to make more precise statements about error probabilities[2] culminated in Gallager's elegant derivation[3] of an exponential upper bound on attainable error probabilities, and in a nearly identical lower bound.[4]



$\Lambda_m \bigcap \Lambda_k = \emptyset$
$\bigcup_m \Lambda_m = \mathcal{Y}^n$

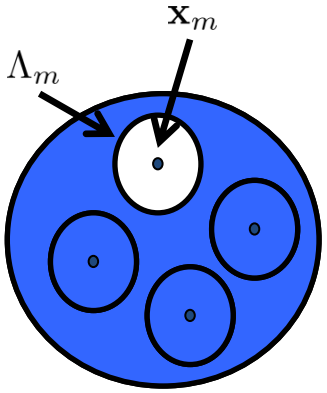
$\Lambda_m \bigcap \Lambda_k = \emptyset$
$\bigcup_m \Lambda_m \subseteq \mathcal{Y}^n$

$\Lambda_m \bigcap \Lambda_k \neq \emptyset$
$\bigcup_m \Lambda_m \subseteq \mathcal{Y}^n$

Error probabilities

Block error probability

$$P_{\mathrm{e}|m} = \sum_{\mathbf{y} \in \Lambda_m^{\mathrm{c}}} p(\mathbf{y}|\mathbf{x}_m)$$



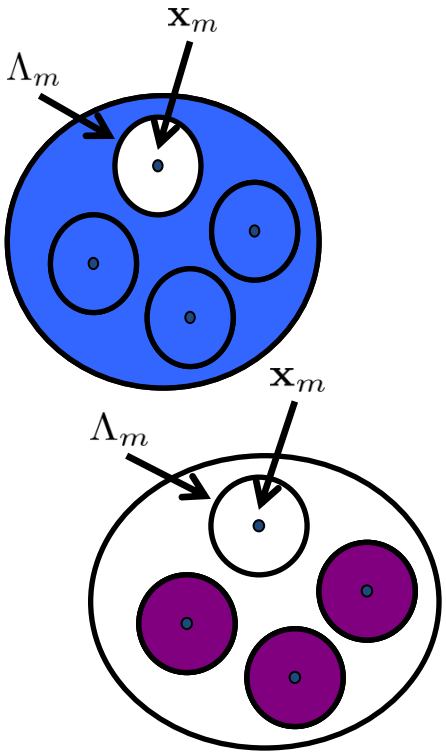
Error probabilities

Block error probability

$$P_{\mathrm{e}|m} = \sum_{\mathbf{y} \in \Lambda_m^{\mathrm{c}}} p(\mathbf{y}|\mathbf{x}_m)$$

Undetected error probability

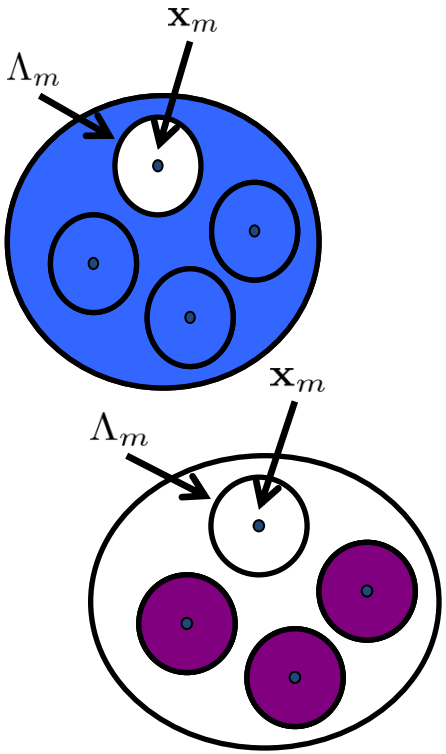
$$P_{\mathrm{ue}|m} = \sum_{m' \neq m} \sum_{\mathbf{y} \in \Lambda_{m'}} p(\mathbf{y}|\mathbf{x}_m)$$



Error probabilities

Block error probability

$$P_{\mathrm{e}|m} = \sum_{\mathbf{y} \in \Lambda_m^{\mathrm{c}}} p(\mathbf{y}|\mathbf{x}_m)$$



Undetected error probability

$$P_{\mathrm{ue}|m} = \sum_{m' \neq m} \sum_{\mathbf{y} \in \Lambda_{m'}} p(\mathbf{y}|\mathbf{x}_m)$$

Erasure probability

$$P_{\mathrm{x}|m} = P_{\mathrm{e}|m} - P_{\mathrm{ue}|m}$$

Error probabilities

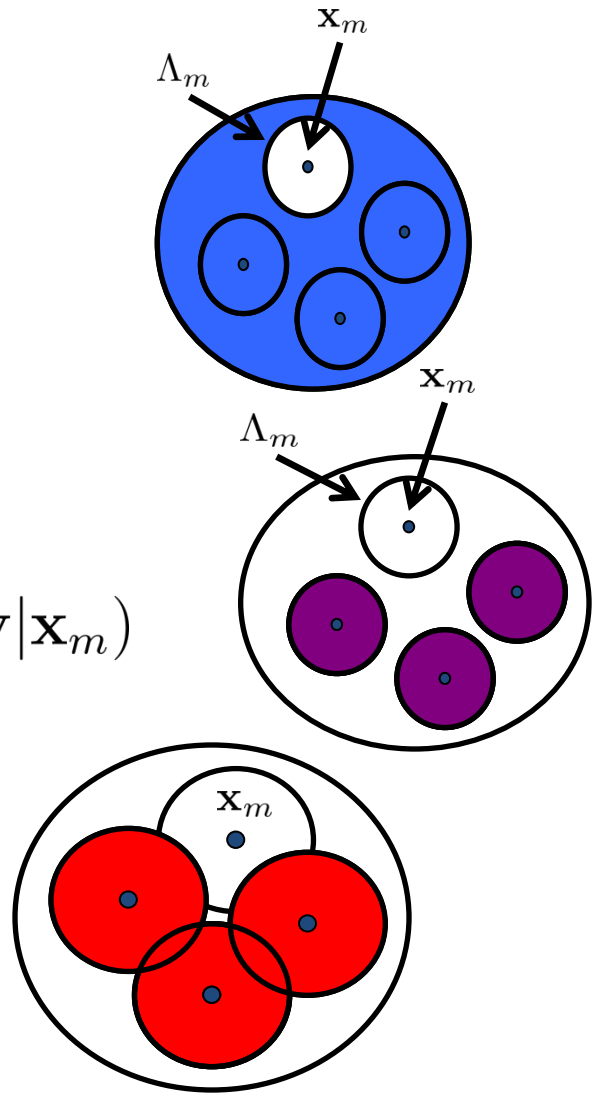
Block error probability

$$P_{\mathrm{e}|m} = \sum_{\mathbf{y} \in \Lambda_m^{\mathrm{c}}} p(\mathbf{y}|\mathbf{x}_m)$$

Undetected error probability

$$P_{\mathrm{ue}|m} = \sum_{m' \neq m} \sum_{\mathbf{y} \in \Lambda_{m'}} p(\mathbf{y}|\mathbf{x}_m)$$

Expected number of incorrect codewords



Optimal decoding

$$\Lambda_m = \left\{ \mathbf{y} \in \mathcal{Y}^n : \ \frac{\Pr(\mathbf{y}, \mathbf{x}_m)}{\sum_{m' \neq m} \Pr(\mathbf{y}, \mathbf{x}_{m'})} \geq e^{nT} \right\}$$

Chapter 4: "Optimal generalized decoding of convolutional codes," *Proceedings of the Tenth International Symposium on Communication Theory and Applications, pp. 6–10, Ambleside, UK, July 2009*

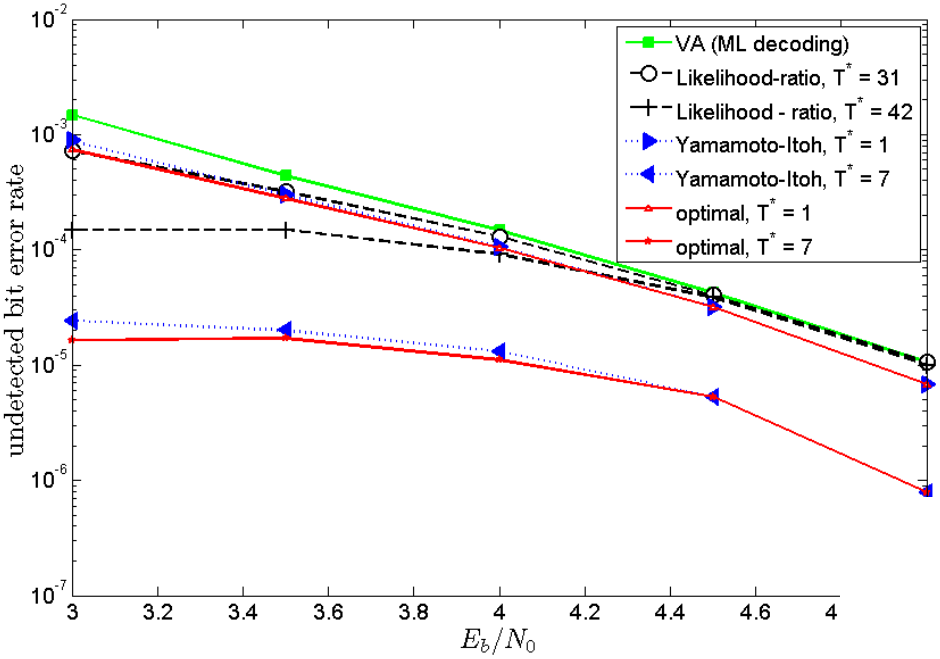
Optimal generalized decoding of convolutional codes

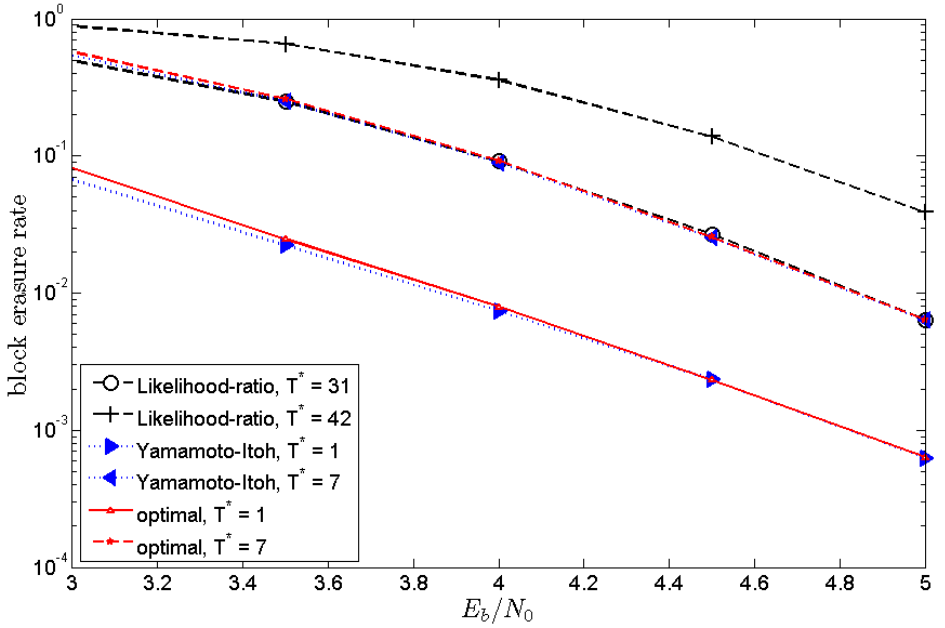
- Via the BCJR algorithm

$$\frac{\Pr(\mathbf{y}, \mathbf{x}_m)}{\sum_{m' \neq m} \Pr(\mathbf{y}, \mathbf{x}_{m'})} = \frac{\Pr(\mathbf{y}, \mathbf{x}_m)}{\Pr(\mathbf{y}) - \Pr(\mathbf{y}, \mathbf{x}_m)}$$

- Via the VA
  - path and branch metrics: standard add-compare-select
  - recursive evaluation of the denuminator via the generalized metrics
    - Multiply by the branch metric (addition)
    - Add the not survived metrics
- Channel state information at the RX

Example

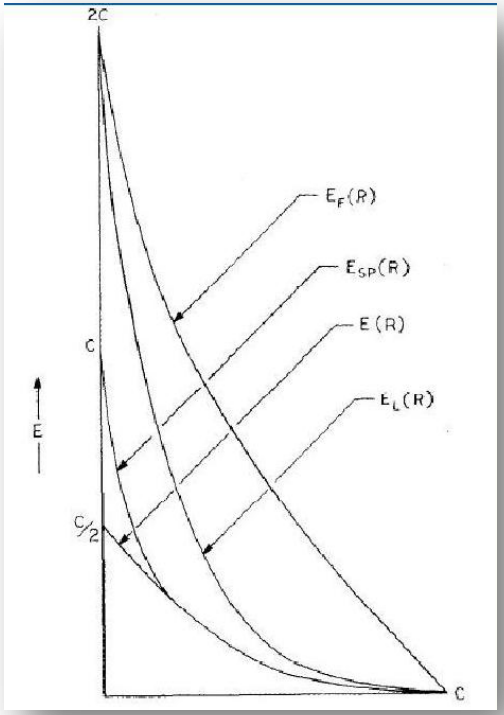

VA (ML decoding)
Likelihood-ratio, T* = 31
Likelihood - ratio, T* = 42
Yamamoto-Itoh, T* = 1
Yamamoto-Itoh, T* = 7
optimal, T* = 1
optimal, T* = 7
undetected bit error rate
E_b/N_0


Likelihood-ratio, T* = 31
Likelihood-ratio, T* = 42
Yamamoto-Itoh, T* = 1
Yamamoto-Itoh, T* = 7
optimal, T* = 1
optimal, T* = 7
block erasure rate
E_b/N_0

Optimal decoding

$$\Lambda_m = \left\{ \mathbf{y} \in \mathcal{Y}^n : \ \frac{\Pr(\mathbf{y}, \mathbf{x}_m)}{\sum_{m' \neq m} \Pr(\mathbf{y}, \mathbf{x}_{m'})} \geq e^{nT} \right\}$$

Error exponents for feedback schemes



Message independence for generalized decoding

Proposition

A1. Linear block codes

A2. Memoryless symmetric channels

The block error probability and undetected error probability under Forney's optimal decoding rule are independent of the transmitted message.

For list decoding: the block error probability and the average number of incorrect codewords are independent of the transmitted message.

Similar propositions for LR test and fixed-size list-decoding.

Block codes under optimal decoding

Proposition:

$$P_{\mathrm{e}|m} \leq e^{nsT} D_{\mathrm{B}}(m, G_n^m, s, \rho)$$

$$P_{\mathrm{ue}} \leq e^{n(s-1)T} \frac{1}{M} \sum_{m=1}^{M} D_{\mathrm{B}}(m, G_n^m, s, \rho), \quad s \geq 0, \quad 0 \leq \rho \leq 1$$

$$D_{\mathrm{B}}(m, G_n^m, s, \rho) = \left(\sum_{\mathbf{y}} G_n^m(\mathbf{y}) p(\mathbf{y}|\mathbf{x}_m) \right)^{1-\rho} \left(\sum_{m' \neq m} \sum_{\mathbf{y}} p(\mathbf{y}|\mathbf{x}_m) G_n^m(\mathbf{y})^{1-\frac{1}{\rho}} \left(\frac{p(\mathbf{y}|\mathbf{x}_{m'})}{p(\mathbf{y}|\mathbf{x}_m)} \right)^{\frac{s}{\rho}} \right)^{\rho}$$

Block codes under optimal decoding

Proposition:

$$P_{\mathrm{e}|m} \leq e^{nsT} D_{\mathrm{B}}(m, G_n^m, s, \rho)$$

$$P_{\mathrm{ue}} \leq e^{n(s-1)T} \frac{1}{M} \sum_{m=1}^{M} D_{\mathrm{B}}(m, G_n^m, s, \rho), \quad s \geq 0, \quad 0 \leq \rho \leq 1$$

Corollary (random coding):

$$P_{\mathrm{e}} \leq e^{-nE_1(R,T)}$$

$$P_{\mathrm{ue}} \leq e^{-nE_2(R,T)}$$

Linear block codes
Memoryless symmetric channels
Optimal decoding

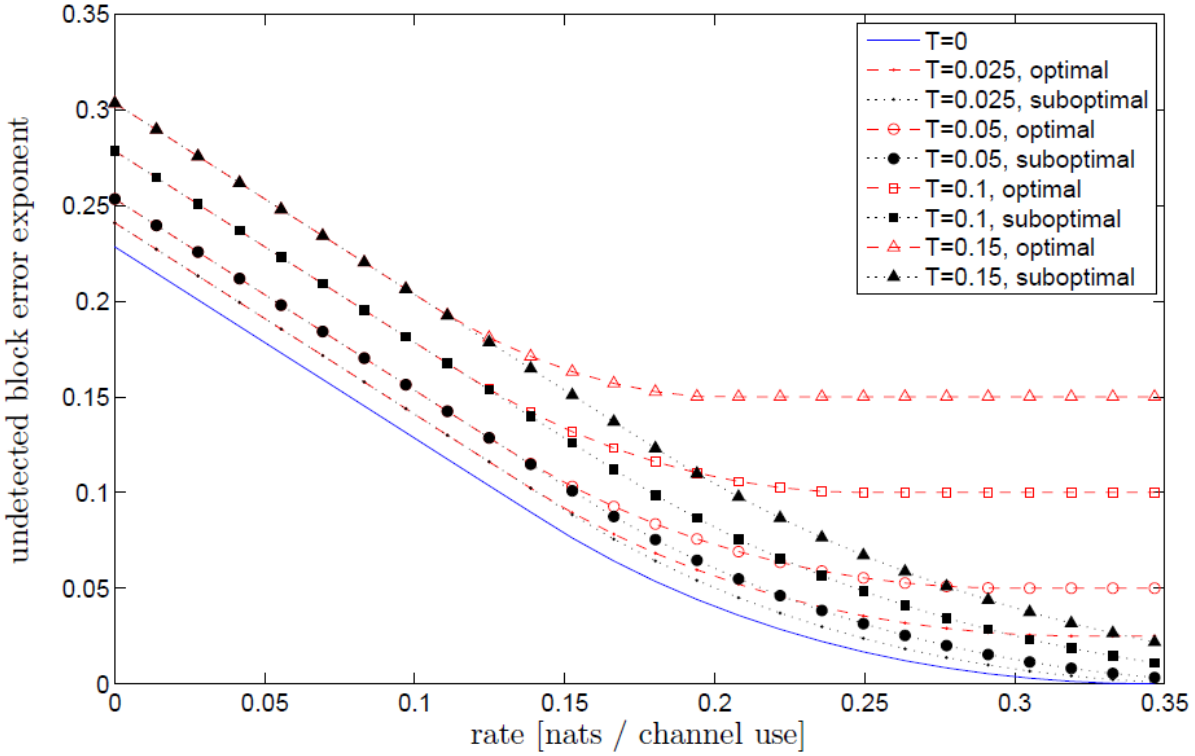
$$P_{\mathrm{e}} \leq e^{-n\left(E(\rho,R,\mathcal{C})-\frac{\rho T}{1+\rho}\right)}, \quad P_{\mathrm{ue}} \leq e^{-n\left(E(\rho,R,\mathcal{C})+\frac{T}{1+\rho}\right)}$$

$$E\left(\rho,R,\mathcal{C}\right) \triangleq E_0(\rho) - \rho\left(R + \frac{\ln(\alpha(\mathcal{C}))}{n}\right)$$

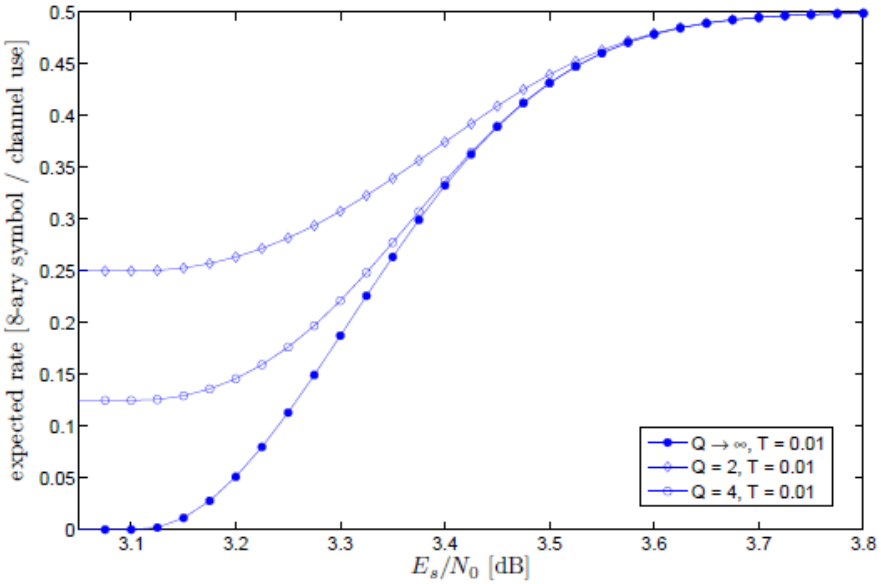
$$E_0\left(\rho\right) \triangleq -\ln\left(\sum_y \left(\frac{1}{2}p(y|0)^{\frac{1}{1+\rho}} + \frac{1}{2}p(y|1)^{\frac{1}{1+\rho}}\right)^{1+\rho}\right)$$

$$\alpha(\mathcal{C}) \triangleq \max_{1\leq i\leq n} \frac{|\mathcal{C}_i|}{2^{-(n-k)}\binom{n}{i}}$$

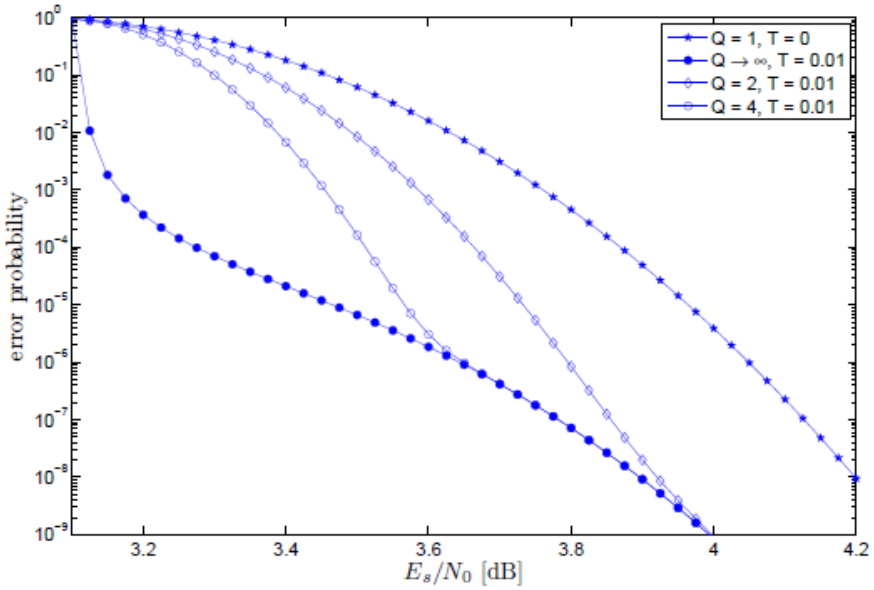
Example


undetected block error exponent
rate [nats / channel use]
0
0.05
0.1
0.15
0.2
0.25
0.3
0.35
T=0
T=0.025, optimal
T=0.025, suboptimal
T=0.05, optimal
T=0.05, suboptimal
T=0.1, optimal
T=0.1, suboptimal
T=0.15, optimal
T=0.15, suboptimal

Performance of Feedback schemes



(a) Lower bounds on the expected rates

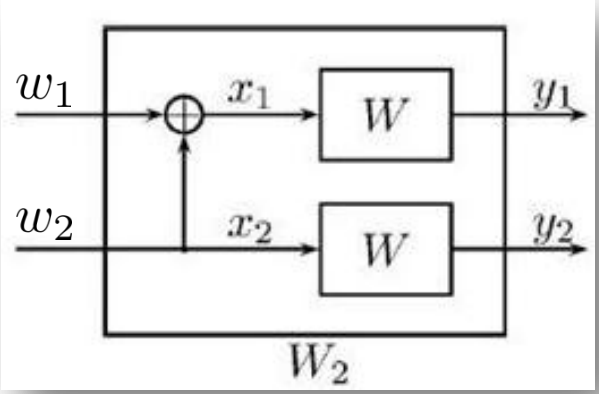


(b) Upper bounds on the error probability

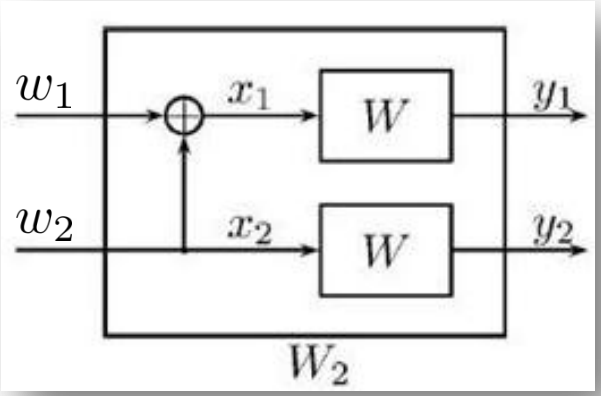
Polar codes

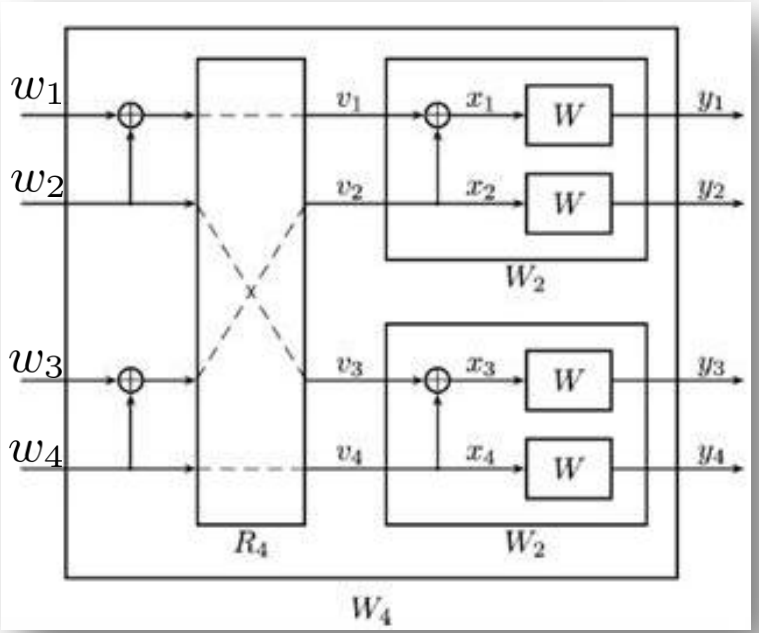
- Arikan, IEEE IT July 2009
- Arikan and Telatar, ISIT 2009
- Korada and Urbanke, IEEE IT, April 2010

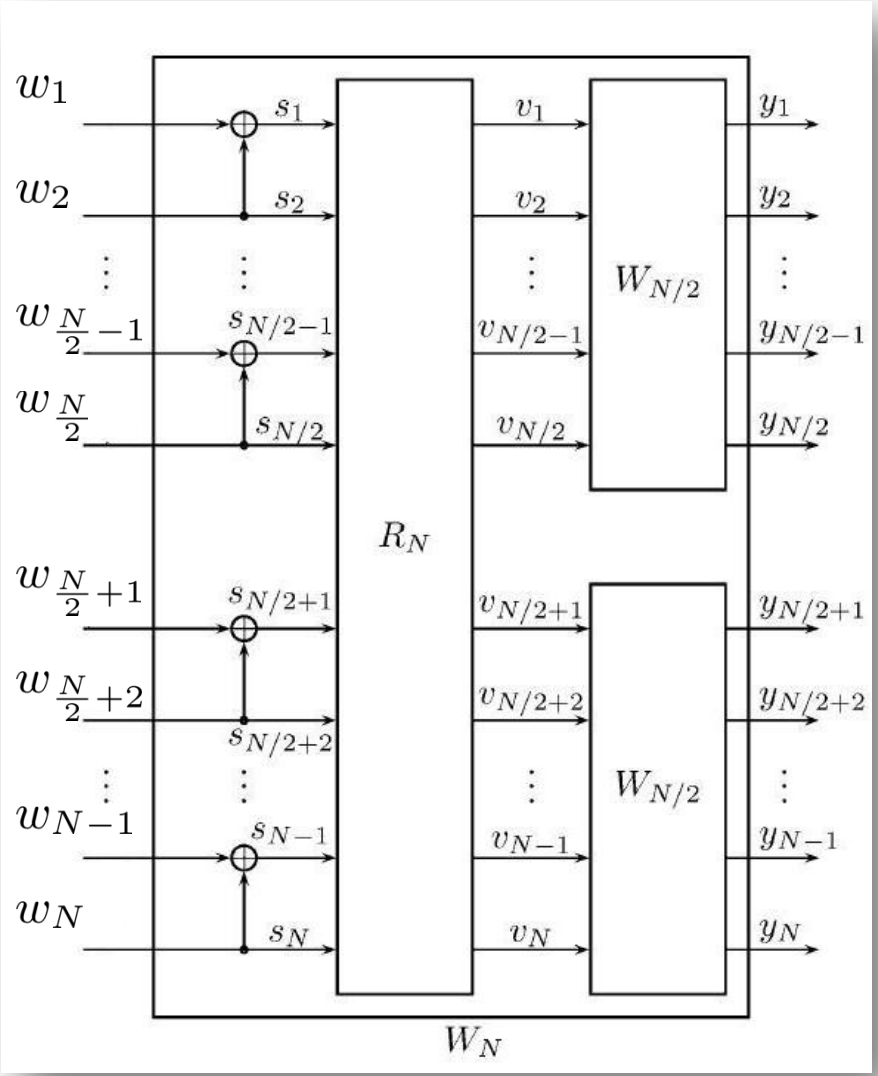
Recursive definition of polar codes



Recursive definition of polar codes







Combined channels and information sets

Combined channels

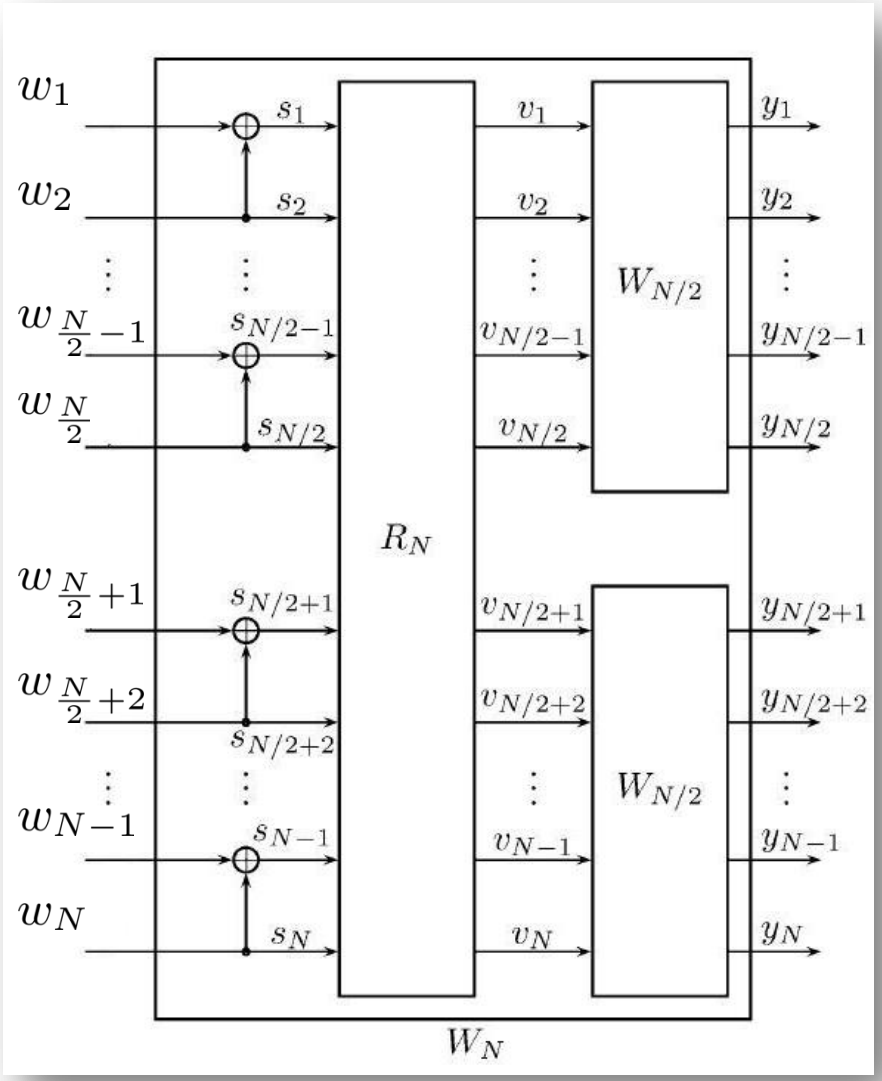
$$W_N(\mathbf{y}|\mathbf{w})$$

Information bits:

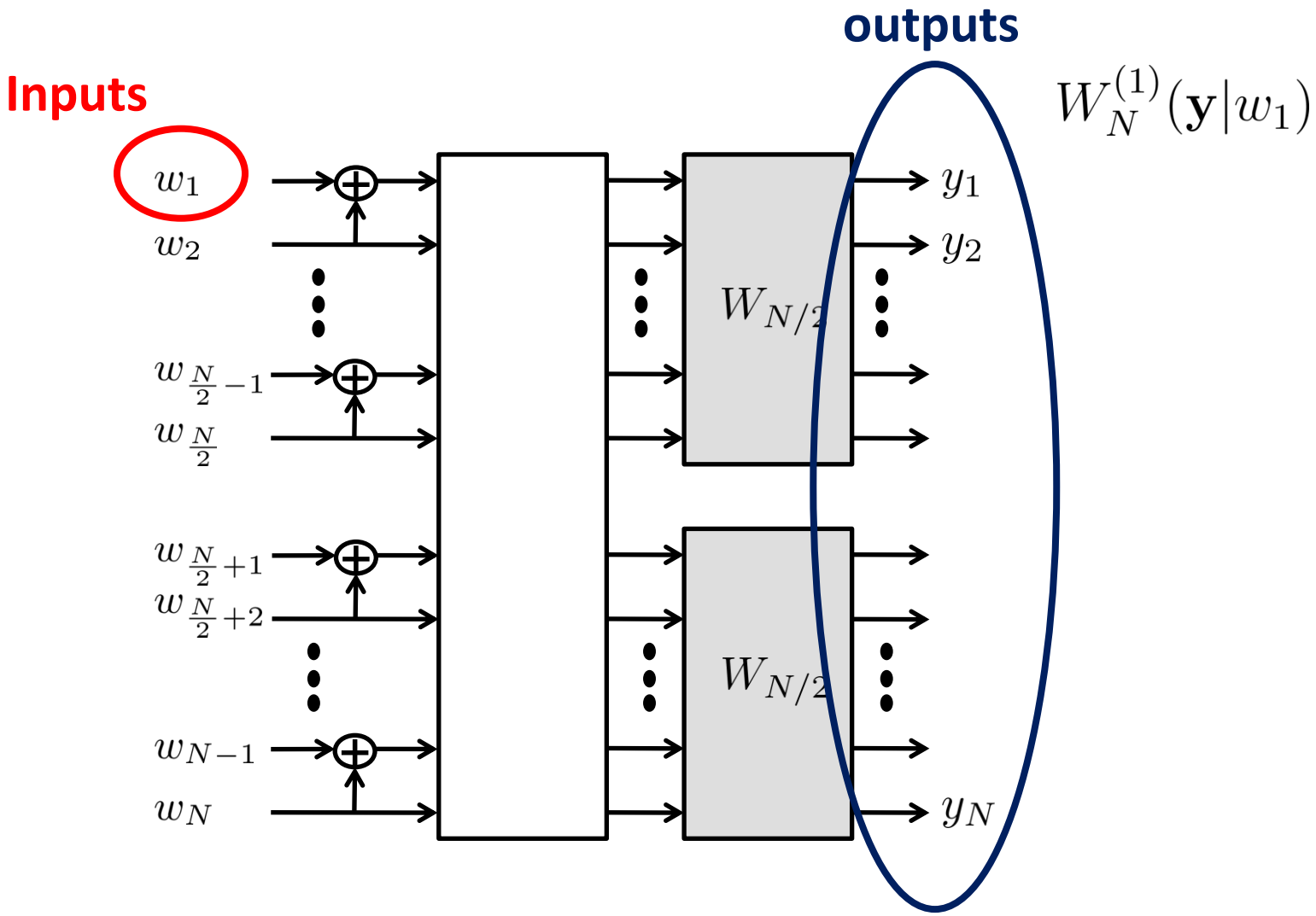
$$w_i, \quad i \in \mathcal{A}$$

Pre-determined bits

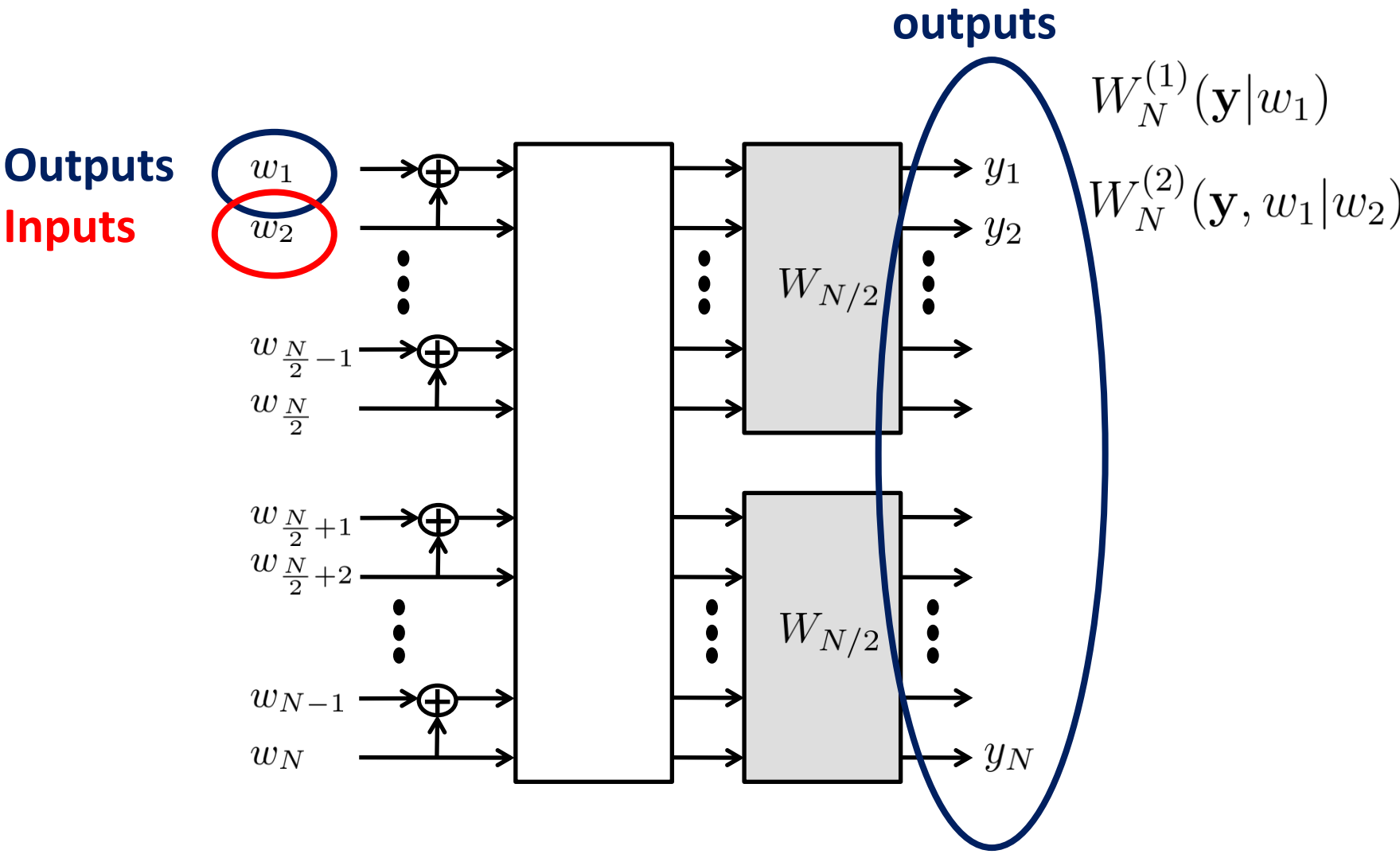
$$w_i, \quad i \notin \mathcal{A}$$



Split channels



Split channels

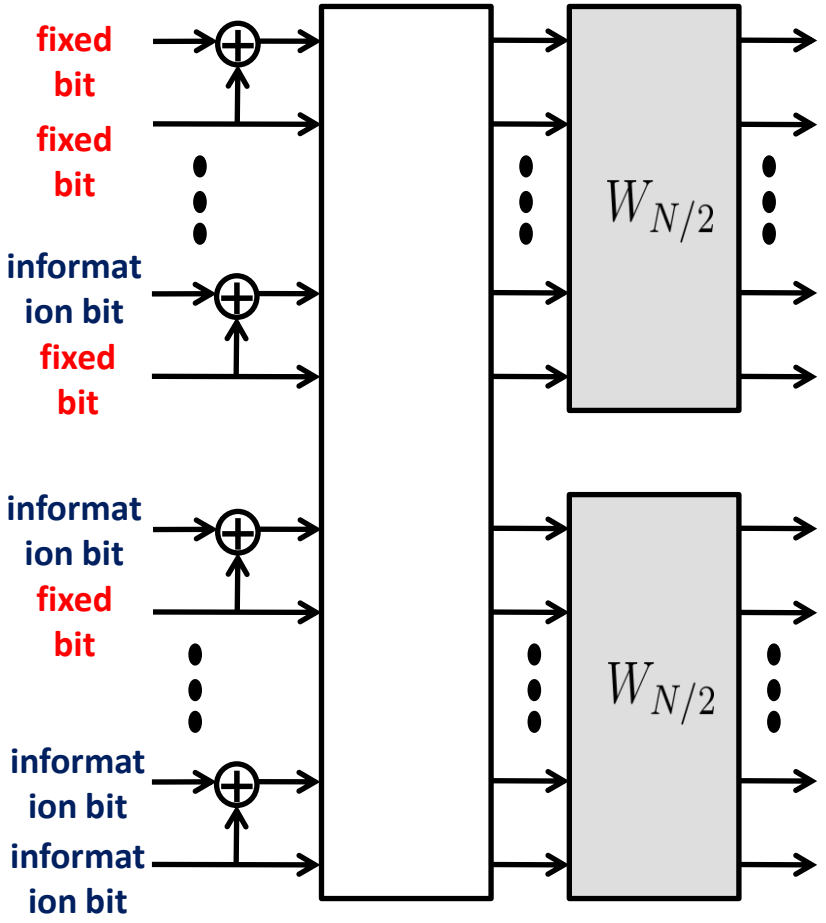


The ‘magic’ of channel polarization

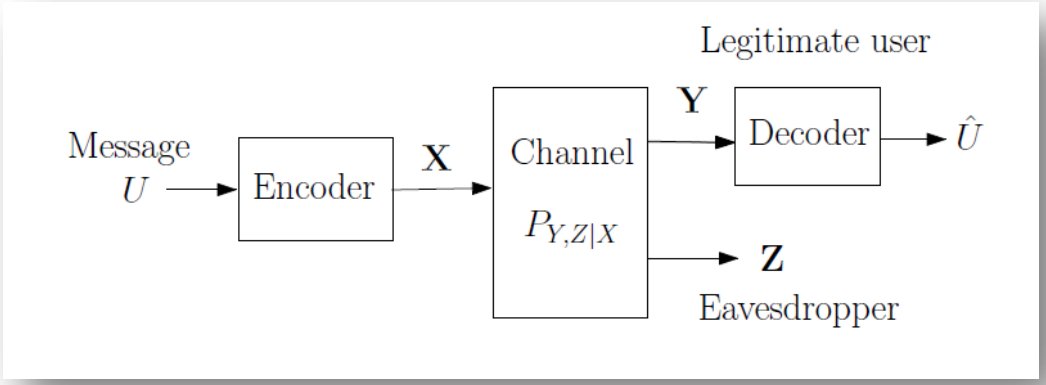
Magic no. 1:
The split channels polarize
to perfect or nothing

Magic no. 2:
There are enough “good” indices
The symmetric capacity is achievable
index ordering is non-trivial and non-consecutive

Magic no. 3:
Successive cancellation decoding



Chapter 5: Polar coding for the wiretap channel



Achievable rates (R, R_{e})

$$P_{\mathrm{e}} \to 0$$

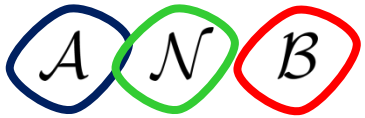
$$R_{\mathrm{e}} \leq \lim_{N\to\infty} \frac{1}{N} H(U|\mathbf{Z})$$

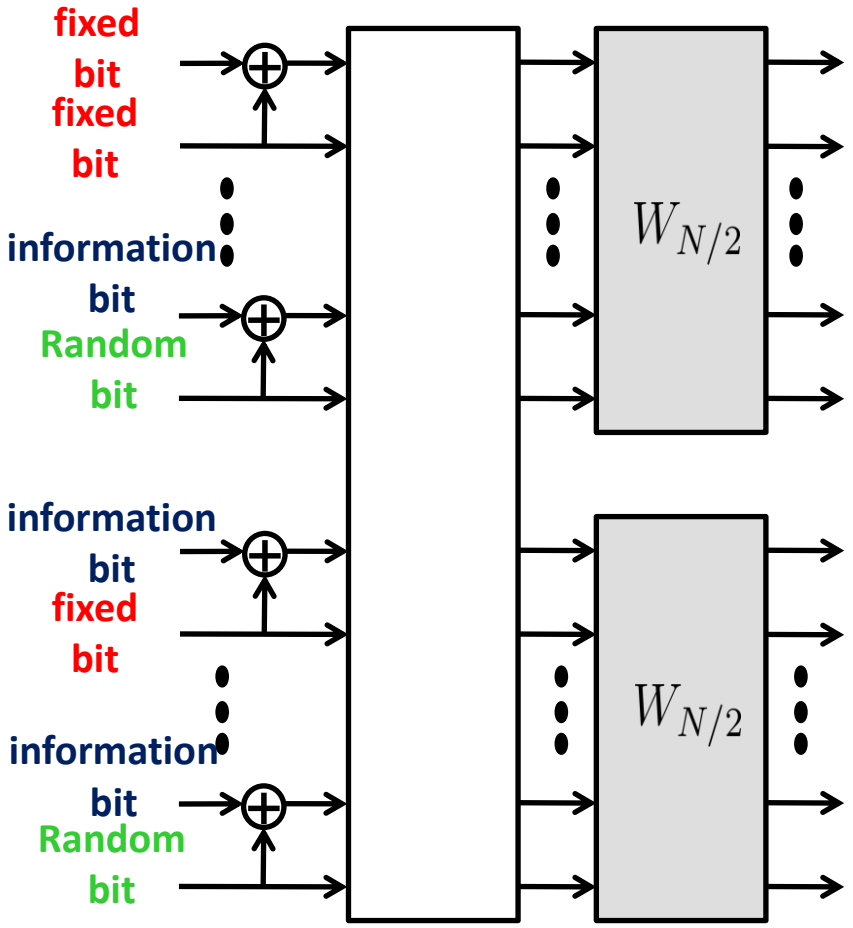
Theorem: For symmetric and degraded channels

$$\left\{ (R, R_{\mathrm{e}}) : \begin{array}{l} 0 \leq R \leq C(P_{Y|X}) \\ 0 \leq R_{\mathrm{e}} \leq R \\ R_{\mathrm{e}} \leq C(P_{Y|X}) - C(P_{Z|X}) \end{array} \right\}$$

Polar secrecy encoding

Index sets





A secrecy achieving property

Theorem (physically-degraded and symmetric wire-tap channels)

$$R < C(P_{Y|X}) - C(P_{Z|X})$$

$$\exists\ \mathcal{A},\ \ \mathcal{N} \qquad\qquad R \leq \frac{1}{N}|\mathcal{A}_N|$$

$$\lim_{n\to\infty} \frac{1}{N} H(U|\mathbf{Z}) \geq R$$

$$P_{\mathrm{e}} \to o$$

Secrecy achieving polar coding

Index sets

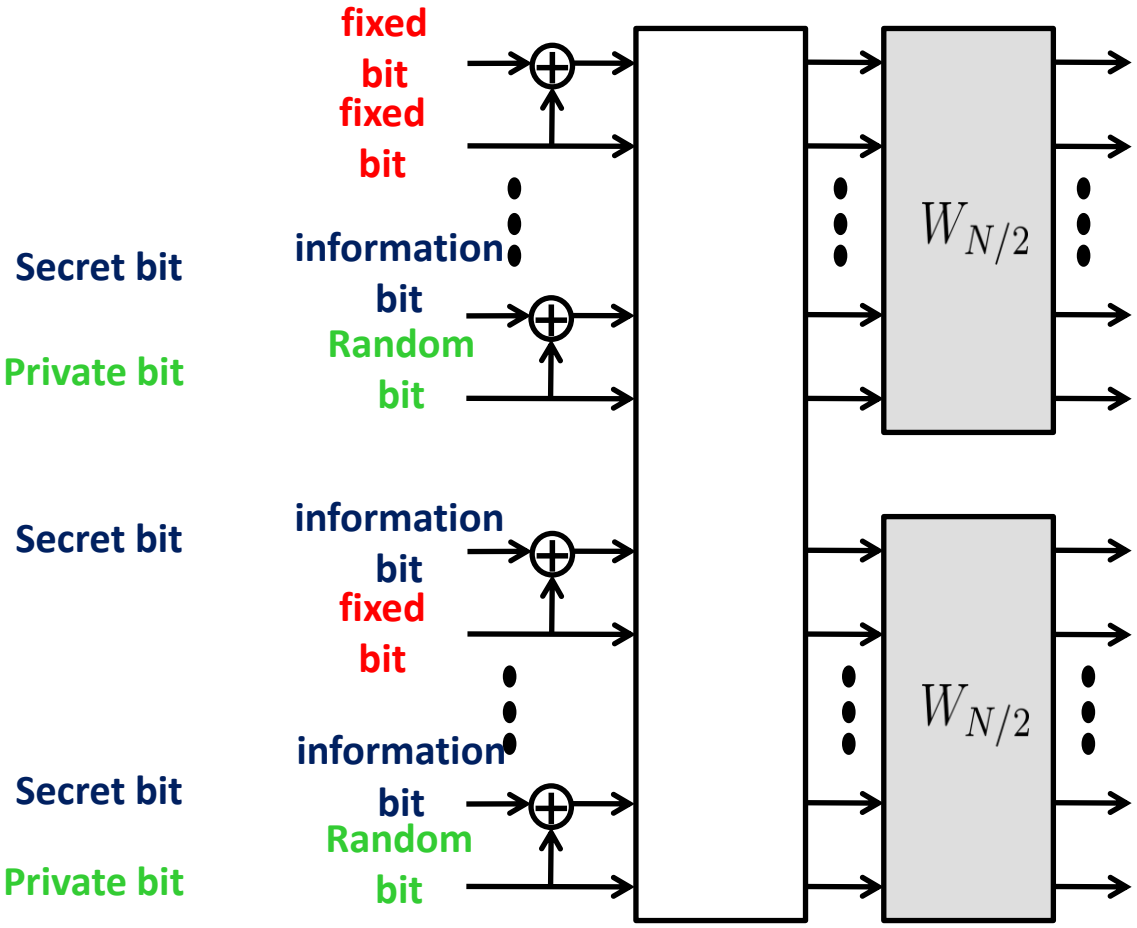
Good for both $\mathcal{N}$

Good only for the legitimate $\mathcal{A}$

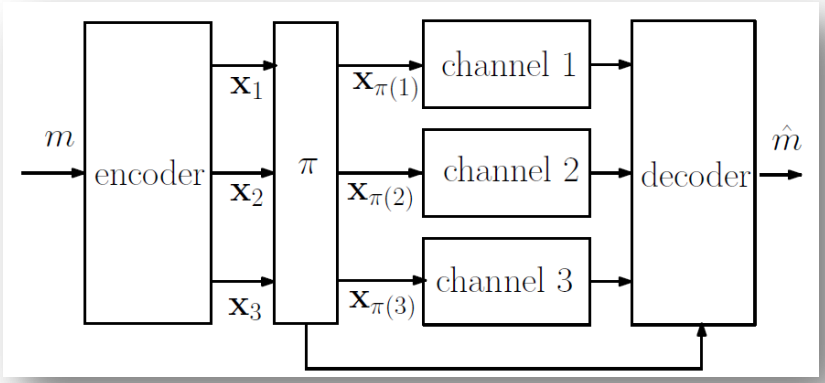
The rest $\mathcal{B}$

1. A Polarization argument for the set sizes
2. Successive decoding for the legitimate user
3. Analysis of the equivocation rate – based on Fano's inequality

Secret and private messages with polar coding



Chapter 6: Polar coding for Arbitrarily Permuted Parallel Channels



Achievable rates:

$$\frac{1}{n}\log_2 M \geq R - \delta$$
$$P_{\mathrm{e}}^{(\pi)}(n) \leq \delta, \ \forall \pi : [S] \to [S]$$

Theorem (Willems and Gorokhov):

$$C_{\Pi} = \sum_{s=1}^{S} C_s$$

Monotone index sets

Corollary:

Binary –input memoryless degraded symmetric channels.

$$C_1 \geq C_2 \geq \cdots \geq C_S.$$

Rates:

$$0 \leq R_s \leq C_s$$

There exists “good” monotone index sets: $\mathcal{A}^{(S)} \subseteq \mathcal{A}^{(S-1)} \subseteq \cdots \subseteq \mathcal{A}^{(1)}$

$$|\mathcal{A}^{(s)}| \geq NR_s$$

Monotone index sets

Polarized for the worse channel: $C_S, \quad R_S, \quad \mathcal{A}^{(S)}$

What is good for the worse, is good for the almost worse

Polarization gives the rest of the "good" indices:

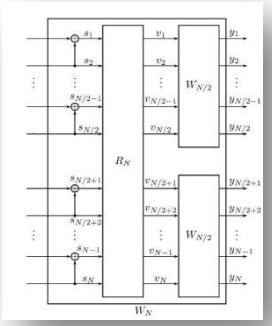
$$\mathcal{A}^{(S)} \subseteq \mathcal{A}^{(S-1)}$$

Repeat this,…Finally: $$\mathcal{A}^{(S)} \subseteq \mathcal{A}^{(S-1)} \subseteq \cdots \subseteq \mathcal{A}^{(1)}$$

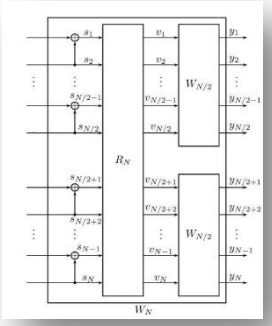
$$|\mathcal{A}^{(s)}| \geq NR_s$$

Parallel polar coding for 2 channels

Channel 1



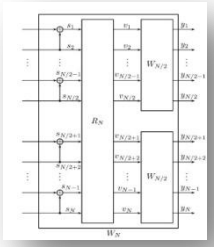
Channel 2



Parallel polar coding for 2 channels

The decoding process for the stronger channel generates the "predetermined and fixed" bits for the degraded channel

Channel 1

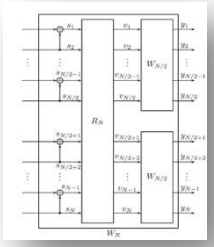


@ receiver 1

Index set design

Received vector

Channel 2



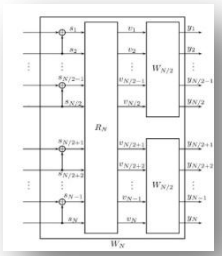
Index set design

Received vector

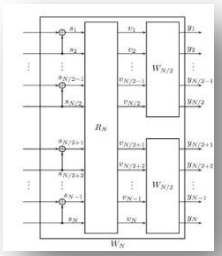
@ receiver 2

Parallel polar coding for 3 channels

Channel 1

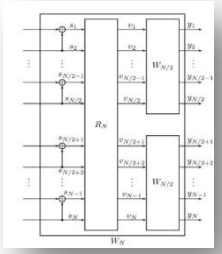


Channel 2



A **repetion code** for the good indices of channel 1 which are not good for channel 2

Channel 3



A **parity check code** for the good indices of channel 2 which are not good for channel 3

Encoding and decoding for 3 channels

$$\mathbf{x}_1 = \mathbf{u}_{1,1} G_n\left(\mathcal{A}_n^{(3)}\right) + \mathbf{u}_{1,2} G_n\left(\mathcal{A}_n^{(2)} \setminus \mathcal{A}_n^{(3)}\right) + \mathbf{u}_{\mathrm{r}} G_n\left(\mathcal{A}_n^{(1)} \setminus \mathcal{A}_n^{(2)}\right) + \mathbf{b} G_b\left([n] \setminus \mathcal{A}_n^{(1)}\right)$$

$$\mathbf{x}_2 = \mathbf{u}_{2,1} G_n\left(\mathcal{A}_n^{(3)}\right) + \mathbf{u}_{2,2} G_n\left(\mathcal{A}_n^{(2)} \setminus \mathcal{A}_n^{(3)}\right) + \mathbf{u}_{\mathrm{r}} G_n\left(\mathcal{A}_n^{(1)} \setminus \mathcal{A}_n^{(2)}\right) + \mathbf{b} G_b\left([n] \setminus \mathcal{A}_n^{(1)}\right)$$

$$\mathbf{x}_3 = \mathbf{u}_3 G_n\left(\mathcal{A}_n^{(3)}\right) + \left(\mathbf{u}_{1,2} + \mathbf{u}_{2,2}\right) G_n\left(\mathcal{A}_n^{(2)} \setminus \mathcal{A}_n^{(3)}\right) + \mathbf{u}_{\mathrm{r}} G_n\left(\mathcal{A}_n^{(1)} \setminus \mathcal{A}_n^{(2)}\right) + \mathbf{b} G_n\left([n] \setminus \mathcal{A}_n^{(1)}\right)$$

Channel P_1		Channel P_2		Channel P_3	
Transmitted Codeword	Decoded Information	Transmitted Codeword	Decoded Information	Transmitted Codeword	Decoded Information
$\mathbf{x}_1$	$\mathbf{u}_{1,1}, \mathbf{u}_{1,2}, \mathbf{u}_{\mathrm{r}}$	$\mathbf{x}_2$	$\mathbf{u}_{2,1}, \mathbf{u}_{2,2}$	$\mathbf{x}_3$	$\mathbf{u}_3$
		$\mathbf{x}_3$	$\mathbf{u}_3, \mathbf{u}_{1,2} + \mathbf{u}_{2,2}$	$\mathbf{x}_2$	$\mathbf{u}_{2,1}$
$\mathbf{x}_2$	$\mathbf{u}_{2,1}, \mathbf{u}_{2,2}, \mathbf{u}_{\mathrm{r}}$	$\mathbf{x}_1$	$\mathbf{u}_{1,1}, \mathbf{u}_{1,2}$	$\mathbf{x}_3$	$\mathbf{u}_3$
		$\mathbf{x}_3$	$\mathbf{u}_3, \mathbf{u}_{1,2} + \mathbf{u}_{2,2}$	$\mathbf{x}_1$	$\mathbf{u}_{1,1}$
$\mathbf{x}_3$	$\mathbf{u}_3, \mathbf{u}_{1,2} + \mathbf{u}_{2,2}, \mathbf{u}_{\mathrm{r}}$	$\mathbf{x}_1$	$\mathbf{u}_{1,1}, \mathbf{u}_{1,2}$	$\mathbf{x}_2$	$\mathbf{u}_{2,1}$
		$\mathbf{x}_2$	$\mathbf{u}_{2,1}, \mathbf{u}_{2,2}$	$\mathbf{x}_1$	$\mathbf{u}_{1,1}$

The general case

- Theorem (MDS codes):

  For an MDS code of dimension k every k symbols completely characterize the codeword
- Combined MDS & Polar codes for the genral degraded case
- The proposed technique does not achieve the capacity in the non-degraded case

Non-degraded parallel channels

- The worst Bhattacharyya parameter whole the split channels
- A parallel polarization based on the corresponding erasure channels

$$S - \sum_{s=1}^{S} B(P_s)$$

- Upper and (improved) lower bounds based on a compound setting

Upper and lower bounds

- A lower bound for the compound setting

$$C\big(\{P_s\}_{s\in[S]}\big) \geq 1 - \frac{1}{2^k} \sum_{\sigma\in\{0,1\}^k} \max_{s\in[S]} B\big(P_s^\sigma\big)$$

- A lower bounds for the parallel transmission scheme

$$C(P_{s_S}) + S - 1 - \frac{1}{2^k} \sum_{s\in[S-1]} \sum_{\sigma\in\{0,1\}^k} \max_{i\in\{s,\ldots S\}} B\big(P_{s_i}^\sigma\big).$$

- An Upper bound
- A BSC+BEC Example (0.982 bits per channel use)

Summary

- Performance bounds
  - Non-binary linear block codes under ML decoding
  - Binary and non-binary linear block codes under generalized decoding rules
- Polar coding
  - Wire-tap channel
  - Parallel channels with arbitrary input-permutation